Amendments To Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A method for authenticating data at a server, the method comprising:

   a. receiving a data request from a client;

   b. retrieving data based on the received data request;

   c. upon retrieving the data, formatting the retrieved data in real-time at said server, wherein the formatted data includes at least one authenticity key;

   d. returning the formatted data to the client; and,

   e. facilitating authentication of ~~authenticating~~ the authenticity key to verify the source of the formatted data.

2. (original) The method of Claim 1, wherein the formatted data is a web page.

3. (original) The method of Claim 1, further comprising:

   a. reading the formatted data at the client;

   b. determining if the formatted data includes the at least one authenticity key;

   c. if the formatted data includes the at least one authenticity key;

   d. verifying authenticity based on the at least one authenticity key.

4. (original) The method of Claim 3, further comprising displaying the data based on the verification of the at least one authenticity key.

5. (currently amended) The method of Claim 4, wherein at least one authenticity stamp will be displayed for data that has been successfully verified.

6. (original) The method of Claim 4, wherein one authenticity stamp will be displayed for each graphical image.

7. (original) The method of Claim 4, wherein a non-authenticity stamp will be displayed for data that has not successfully been verified.

8. (currently amended) A system for authenticating data, the system comprising:

a. at least one client;

b. at least one server;

c. a network, wherein the client and the server communicate via the network; and

d. at least one authentication server, wherein said at least one authentication server is in communication with said at least one server, said authentication server being configured to insert an authenticity key <u>in real time</u> into the data requested from said client thereby facilitating said client to authenticate the authenticity key to verify the source of the data.

9. (original) The system of Claim 8, wherein said at least one client includes a browser, wherein pages are displayed to a user on a display device on said at least one client.

10. (original) The system of Claim 8, wherein said at least one server sends a page including an authenticity key to said at least one client.

11. (original) The system of Claim 10, wherein said at least one client verifies authenticity of the page based on the authenticity key.

12. (original) The system of Claim 11, wherein the page is displayed on said client, wherein the display includes an indication of the authenticity of the page.

13. (currently amended) A system for authenticating a web page, the system comprising:

a. at least one client;

b. at least one server, wherein said at least one server sends said web page, wherein the web page includes at least one graphic image and wherein each of said at least one graphic images includes an authenticity key, said server being configured to insert an authenticity key in real time into the web page requested from said client thereby facilitating said client to authenticate the authenticity key to verify the source of the web page; and,

c. a network, wherein the client and the server communicate via the network.

14. (currently amended) In a computer system for authenticating data at a server, a computer-readable medium holding computer executable instructions for performing a method comprising the steps of:

a. receiving a data request from a client;

b. retrieving data based on the received data request;

c. upon retrieving the data, formatting the retrieved data in real-time at said server, wherein the formatted data includes an authenticity key;

d. returning the formatted data to the client; and,

e. facilitating authentication of ~~authenticating~~ the authenticity key to verify the source of the formatted data.

15. (original) The computer system of Claim 14, wherein the formatted data is a web page.

16. (original) The computer system of Claim 14, wherein computer executable instructions further comprise the steps of:

a. reading the formatted data at the client;

b. determining if the formatted data includes the authenticity key;

c. if the formatted data includes the authenticity key;

d. verifying authenticity based on the authenticity key.

17. (original) The computer system of Claim 16, wherein the computer executable instructions further comprise the step of: displaying the data based on the verification of the authenticity.

18. (currently amended) The computer system of Claim 17, wherein ~~an~~ <u>at least one</u> authenticity stamp will be displayed for data that has been successfully verified.

19. (currently amended) The computer system of Claim 17, wherein ~~a~~ <u>at least one</u> non-authenticity stamp will be displayed for data that has not successfully been verified.

20. (previously presented) The method of claim 1, wherein said receiving and returning steps are implemented via at least one of internet, interactive television system, broadband system, regular band system, wireless system, radio transmission, landline phone system, and cellular phone system.

21. (previously presented) The method of claim 1, wherein said step of authenticating the authenticity key to verify the source of the formatted data includes a browser plug-in interfacing with a MIME type to authenticate the formatted data private key.

22. (previously presented) The system of claim 8, wherein said authentication server is configured to authenticate user ID and password.

23. (previously presented) The system of claim 8, wherein said authentication server is configured to sign the web page.

24. (NEW) A method for authenticating data at a server, the method comprising:

receiving a data request from a client;

retrieving data based on the received data request;

upon retrieving the data, determining if said data includes a code which requires said data to be authenticated;

formatting the retrieved data in real-time at said server, wherein the formatted data includes at least one authenticity key;

returning the formatted data to the client; and,

facilitating authentication of the authenticity key to verify the source of the formatted data.

25. (NEW) The method of claim 24 further comprising:

decrypting a preferences key;

decrypting a preferences file using said preferences key;

obtaining instructions within said preferences file; and,

inserting a visual signature into said data based on said instructions stored in said preferences file.

26. (NEW) The method of claim 24 further comprising:

decrypting a preferences key using a master preferences key;

decrypting a preferences file using said preferences key;

obtaining instructions within said preferences file; and,

inserting a visual signature into said data based on said instructions stored in said preferences file.

27. (NEW) The method of claim 1 further comprising:

decrypting a preferences key;

decrypting a preferences file using said preferences key;

obtaining instructions within said preferences file; and, inserting a visual signature into said data based on said instructions stored in said preferences file.

28. (NEW) The method of claim 1 further comprising:

decrypting a preferences key using a master preferences key;

decrypting a preferences file using said preferences key;

obtaining instructions within said preferences file; and,

inserting a visual signature into said data based on said instructions stored in said preferences file.